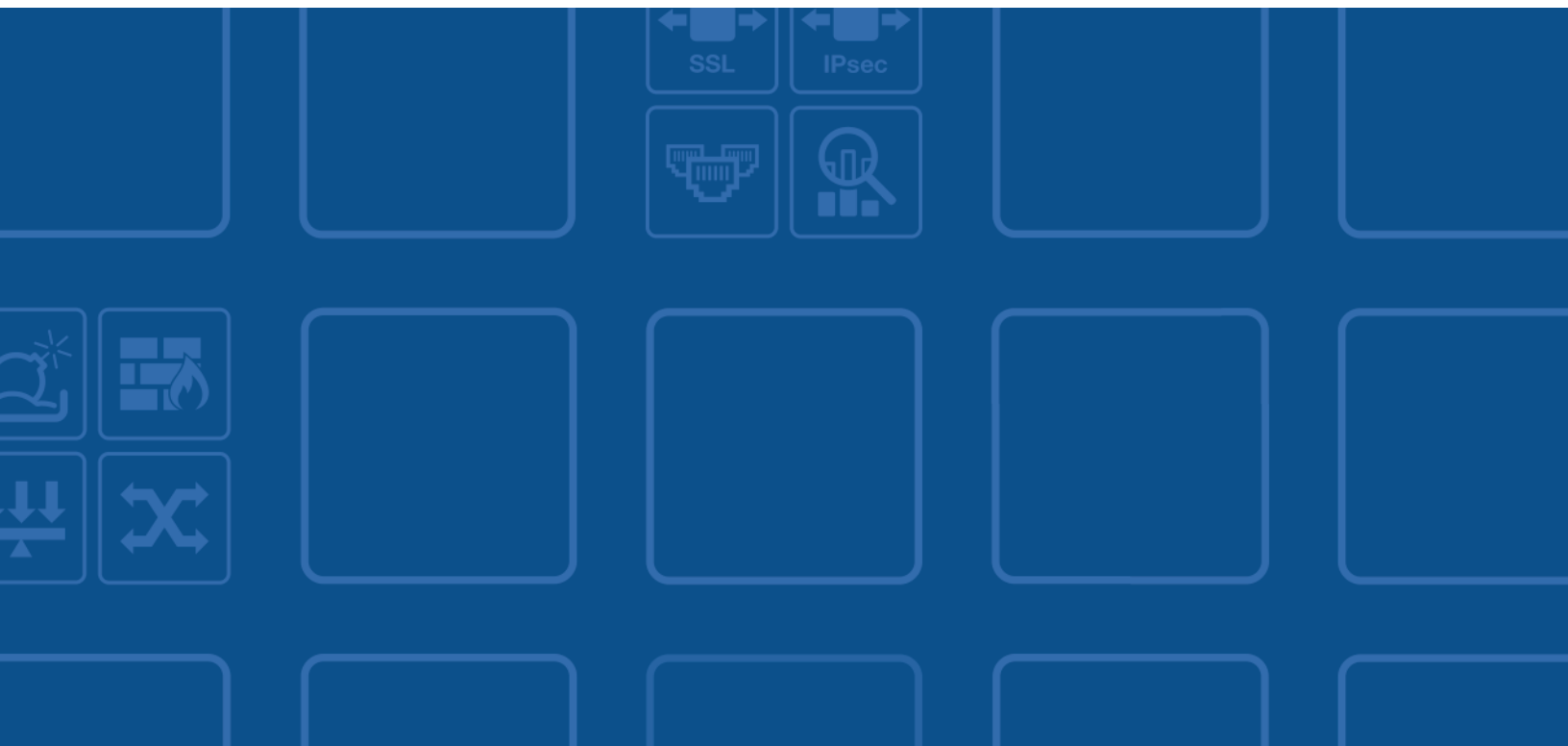
FORTINET
High Performance Network Security

FortiManager - Release Notes

VERSION 5.4.4



FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

July 25, 2018

FortiManager - Release Notes

02-544-450348-20180725

TABLE OF CONTENTS

Change Log

Date	Change Description
2017-10-05	Initial release of 5.4.4.
2017-10-06	Changed 401614 to 442206 in the *Common Vulnerabilities and Exposures* section and added 453371 to *Known Issues*.
2017-10-13	Added 453942 to *Known Issues* > *Device Manager*. Added 450711 to *Known Issues* > *Revision History*.
2017-10-19	Added 422847 to *Resolved Issues* > *Policy and Objects*.
2017-10-20	Added *Product Integration & Support* > *FortiOS/FortiOS Carrier* > *5.4.6*.
2017-10-23	Added 369270 *Known Issues* > *Logging*.
2017-10-24	Added 167355 to *Resolved Issues* > *Policy and Objects*.
2017-10-30	Added note about LENC device support and added 395060 to *Known Issues* > *Device Manager*.
2017-11-14	Added 435256 to *Resolved Issues* > *Device Manager*.
2017-11-20	Added 2.4.0 and 2.4.1 support to *Product Integration & Support* > *FortiSandbox*.
2017-11-30	Added a note to *Upgrade Information*. When upgrading from 5.2, an Import Policy Package should be preformed on all FortiGates using Local-In-Polices.
2017-12-13	Added FortiOS 5.4.7 support to *Product Integration and Support*.
2018-01-10	Added *SFTP Tool* note to *Upgrade Information*.
2018-01-18	Added support for FortiOS 5.4.8.
2018-02-20	Added information about upgrading from 5.2.x.
2018-07-25	Add FMG-300F to *Supported Models* and FAZ-800F to *Product Integration and Support* > *Supported Models* > *FortiAnalyzer models*.

Introduction

This document provides the following information for FortiManager 5.4.4 build 1225:

For more information on upgrading your device, see the FortiManager *Upgrade Guide*.

Supported models

FortiManager version 5.4.4 supports the following models:

FortiManager	FMG-200D, FMG-300D, FMG-300E, FMG-300F, FMG-400E, FMG-1000C, FMG-1000D, FMG-2000E, FMG-3000C, FMG-3000F, FMG-3900E, FMG-4000D, and FMG-4000E.
FortiManager VM	FMG-VM64, FMG-VM64-AWS, FMG-VM64-Azure, FMG-VM64-HV (including Hyper-V 2016), FMG-VM64-KVM, and FMG-VM64-XEN (for both Citrix and Open Source Xen).

What's new in FortiManager 5.4.4

There are no new features or enhancements in FortiManager version 5.4.4.

Special Notices

This section highlights some of the operational changes that administrators should be aware of in 5.4.4.

FortiGate VM 16/32/UL license support

FortiOS 5.4.4 introduces new VM license types to support additional vCPUs. FortiManager 5.4.3 supports these new licenses with the prefixes of FGVM16, FGVM32, and FGVMUL.

Hyper-V FortiManager-VM running on an AMD CPU

A Hyper-V FMG-VM running on a PC with an AMD CPU may experience a kernel panic. Fortinet recommends running VMs on an Intel-based PC.

IPsec connection to FortiOS for logging

FortiManager 5.4.2 with FortiAnalyzer Features enabled no longer supports an IPsec connection with FortiOS 5.0.x/5.2.x. However UDP or TCP + reliable are supported.

Instead of IPsec, you can use the FortiOS reliable logging feature to encrypt logs and send them to FortiManager. You can enable the reliable logging feature on FortiOS by using the `configure log fortianalyzer setting` command. You can also control the encryption method on FortiOS by using the `set enc-algorithm default/high/low/disable` command.

FortiManager 5.4.1 and earlier supports IPsec connection with FortiOS 5.0.x/5.2.x.

VM License (VM-10K-UG) Support

FortiManager 5.4.2 introduces a new VM license (VM-10K-UG) that supports 10,000 devices. It is recommended to upgrade to FortiManager 5.4.2 before applying the new license to avoid benign GUI issues.

If you use the new license with FortiManager 5.4.1 or 5.2.x and earlier, the maximum number of devices is correctly enforced, but the GUI may display some VM information incorrectly. For example, the VM storage maximum may incorrectly display 100GB in the *License Information* widget on the *System Settings* pane. The VM license type may not appear (FortiManager 5.4.1), and the VM license type may show *Unknown* (FortiManager 5.2.9).

System Configuration or VM License is Lost after Upgrade

When upgrading FortiManager from 5.4.0 or 5.4.1 to 5.4.2, it is imperative to reboot the unit before installing the 5.4.2 firmware image. Please see the *FortiManager Upgrade Guide* for details about upgrading. Otherwise, FortiManager may lose system configuration or VM license after upgrade. There are two options to recover the FortiManager unit:

1. Reconfigure the system configuration or add VM license via CLI with `execute add-vm-license <vm license>`.
2. Restore the 5.4.0 backup and upgrade to 5.4.2.

FortiOS 5.4.0 Support

With the enhancement in password encryption, FortiManager 5.4.2 no longer supports FortiOS 5.4.0. Please upgrade FortiGate to 5.4.2.

The following ADOM versions are not affected: 5.0 and 5.2.

Local in-policy after upgrade

After upgrading to FortiManager 5.4.1, you must import or reconfigure local in-policy entries. Otherwise, the subsequent install of policy packages to FortiGate will purge the local in-policy entries on FortiGate.

ADOM for FortiGate 4.3 Devices

FortiManager 5.4 no longer supports FortiGate 4.3 devices. FortiManager cannot manage the devices after the upgrade. To continue managing those devices, please upgrade all FortiGate 4.3 to a supported version, retrieve the latest configuration from the devices, and move the devices to an ADOM database with the corresponding version.

SSLv3 on FortiManager-VM64-AWS

Due to known vulnerabilities in the SSLv3 protocol, FortiManager-VM64-AWS only enables TLSv1 by default. All other models enable both TLSv1 and SSLv3. If you wish to disable SSLv3 support, please run:

```
config system global
   set ssl-protocol t1sv1
end
```

Upgrade Information

Upgrading to FortiManager 5.4.4

You can upgrade FortiManager 5.2.0 or later directly to 5.4.4. If you are upgrading from versions earlier than 5.2.0, you will need to upgrade to FortiManager 5.2 first. (We recommend that you upgrade to 5.2.9, the latest version of FortiManager 5.2.)

Bug ID	Description
404193	ADOM upgrade will fail if the MGMT interface is a dedicated management port and mapped to a dynamic interface. **Workaround**: Before upgrading to 5.4, you should remove MGMT interface from dynamic interface zone, if a managed FortiGate has MGMT interface and if it is a dedicated management port. This is because MGMT interface being set to a dedicated management port cannot be mapped to a dynamic interface zone in 5.4.

When upgrading from FMG 5.2, an *Import Policy Package* should be performed on all FortiGates using *Local-In-Polices*. As of FMG 5.4, these are handled in Policies & Objects.

For details about upgrading your FortiManager device, see the *FortiManager Upgrade Guide*.

During upgrade from 5.2.4 or earlier, invalid dynamic mappings and duplicate package settings are removed from the ADOM database. Please allow sufficient time for the upgrade to complete.

After changing the SFTP tool in FMG 5.4.4, a full directory path may now be required for some servers. Users may need to update their configuration after upgrade.

Previously, the following config example was working:

```
# config system backup all-settings
# set directory "folder/subfolder"
```

After upgrading to 5.4.4, the full path may need to be defined as in the example below:

```
# config system backup all-settings
# set directory "/home/username/folder/subfolder/"
```

The CLI command for manual backup is also affected.
Previously, it was working with:

```
# exec backup all-settings sftp 000.000.000.000
    folder/subfolder/ username password
```

After upgrading to 5.4.4:

```
# exec backup all-settings sftp 000.000.000.000
    /home/username/folder/subfolder/ username password
```

Upgrading from 5.2.x

Starting with FortiManager 5.4.0, you can create a maximum number of Global and ADOM objects for each object category, and the maximum is enforced. The maximum numbers are high and unlikely to be met. The purpose of the maximum is to help avoid excessive database sizes, which can impact performance.

During upgrade from FortiManager 5.2.x to 5.4.x to 5.6.2, objects are preserved, even if the 5.2 ADOM contains more than the maximum number of allowed objects. If you have met the maximum number of allowed objects, you cannot add additional objects after upgrading to FortiManager 5.6.2.

Following are examples of object limits:

- Firewall service custom: 8192 objects
- Firewall service group: 2000 objects

If you have reached the maximum number of allowed objects, you can reduce the number of objects by deleting duplicate or obsolete objects from the ADOM.

You can also reach the maximum number of allowed objects if you have multiple FortiGate/VDOMs in the same ADOM.

You can reduce the number of objects by moving the FortiGates/VDOMs into different ADOMs.

Downgrading to previous firmware versions

FortiManager does not provide a full downgrade path. You can downgrade to a previous firmware release via the GUI or CLI, but doing so results in configuration loss. A system reset is required after the firmware downgrading process has completed. To reset the system, use the following CLI commands via a console port connection:

```
execute reset {all-settings | all-except-ip}
execute format {disk | disk-ext4 | disk-ext3}
```

FortiManager VM firmware

Fortinet provides FortiManager VM firmware images for Amazon AWS, Citrix and Open Source XenServer, Linux KVM, Microsoft Hyper-V Server, and VMware ESX/ESXi virtualization environments.

Amazon Web Services

- The 64-bit Amazon Machine Image (AMI) is available on the AWS marketplace.

Citrix XenServer and Open Source XenServer

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiManager VM installation.
- `.out.OpenXen.zip`: Download the 64-bit package for a new FortiAnalyzer VM installation. This package contains the QCOW2 file for the Open Source Xen Server.
- `.out.CitrixXen.zip`: Download the 64-bit package for a new FortiManager VM installation. This package contains the Citrix XenServer Virtual Appliance (XVA), Virtual Hard Disk (VHD), and OVF files.

Linux KVM

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiManager VM installation.
- `.out.kvm.zip`: Download the 64-bit package for a new FortiManager VM installation. This package contains QCOW2 that can be used by qemu.

Microsoft Azure

The files for Microsoft Azure have AZURE in the filenames, for example `FMG_VM64_AZURE-v<number>-build<number>-FORTINET.out.hyperv.zip`.

- `.out`: Download the firmware image to upgrade your existing FortiManager VM installation.
- `.hyperv.zip`: Download the package for a new FortiManager VM installation. This package contains a Virtual Hard Disk (VHD) file for Microsoft Azure.

Microsoft Hyper-V Server

The files for Microsoft Hyper-V Server have HV in the filenames, for example, `FMG_VM64_HV-v<number>-build<number>-FORTINET.out.hyperv.zip`.

- `.out`: Download the firmware image to upgrade your existing FortiManager VM installation.
- `.hyperv.zip`: Download the package for a new FortiManager VM installation. This package contains a Virtual Hard Disk (VHD) file for Microsoft Hyper-V Server.

Microsoft Hyper-V 2016 is supported.

VMware ESX/ESXi

- `.out`: Download the 64-bit firmware image to upgrade your existing VM installation.
- `.ovf.zip`: Download either the 64-bit package for a new VM installation. This package contains an Open Virtualization Format (OVF) file for VMware and two Virtual Machine Disk Format (VMDK) files used by the OVF file during deployment.

For more information see the FortiManager product data sheet available on the Fortinet web site, http://www.-fortinet.com/products/fortimanager/virtualappliances.html. VM installation guides are available in the Fortinet Document Library.

Firmware image checksums

The MD5 checksums for all Fortinet software and firmware releases are available at the Customer Service & Support portal, https://support.fortinet.com. After logging in select *Download* > *Firmware Image Checksums*, enter the image file name including the extension, and select *Get Checksum Code*.

SNMP MIB files

You can download the *FORTINET-FORTIMANAGER-FORTIANALYZER.mib* MIB file in the firmware image file folder. The Fortinet Core MIB file is located in the main FortiManager version 5.00 file folder.

Product Integration and Support

FortiManager 5.4.4 support

The following table lists 5.4.4 product integration and support information:

Web Browsers	• Microsoft Internet Explorer version 11 or Edge 40 Due to limitation on Microsoft Internet Explorer or Edge, it may not completely render a page with a large set of policies or objects. • Mozilla Firefox version 55 • Google Chrome version 61 Other web browsers may function correctly, but are not supported by Fortinet.

FortiOS/FortiOS Carrier	• 5.4.8 FortiManager 5.4.4 is fully tested as compatible with FortiOS/FortiOS Carrier 5.4.8, with some minor interoperability issues. For information, see Compatibility issues with FortiOS 5.4.8 on page 27. • 5.4.7 • 5.4.6 • 5.4.5 FortiManager 5.4.4 is fully tested as compatible with FortiOS/FortiOS Carrier 5.4.5, with some minor interoperability issues. For information, see Compatibility issues with FortiOS 5.4.5 on page 27. • 5.4.4 FortiManager 5.4.4 is fully tested as compatible with FortiOS/FortiOS Carrier 5.4.4, with some minor interoperability issues. For information, see Compatibility issues with FortiOS 5.4.4 on page 27. • 5.4.1 to 5.4.3 • 5.2.8 to 5.2.11 FortiManager 5.4.4 is fully tested as compatible with FortiOS/FortiOS Carrier 5.2.10, with some minor interoperability issues. For information, see Compatibility issues with FortiOS 5.2.10 on page 28. • 5.2.7 FortiManager 5.4.4 is fully tested as compatible with FortiOS/FortiOS Carrier 5.2.7, with some minor interoperability issues. For information, see Compatibility issues with FortiOS 5.2.7 on page 28. • 5.2.6 FortiManager 5.4.4 is fully tested as compatible with FortiOS/FortiOS Carrier 5.2.6, with some minor interoperability issues. For information, see Compatibility issues with FortiOS 5.2.6 on page 28. • 5.2.2 to 5.2.5 • 5.2.1 FortiManager 5.4.4 is fully tested as compatible with FortiOS/FortiOS Carrier 5.2.1, with some minor interoperability issues. For information, see Compatibility issues with FortiOS 5.2.1 on page 28. • 5.2.0 FortiManager 5.4.4 is fully tested as compatible with FortiOS/FortiOS Carrier 5.2.0, with some minor interoperability issues .For information, see Compatibility issues with FortiOS 5.2.0 on page 29. • 5.0.4 to 5.0.14 FortiManager 5.4.4 is fully tested as compatible with FortiOS/FortiOS Carrier 5.0.4 to 5.0.14, with some minor interoperability issues. For information, see Compatibility issues with FortiOS 5.0.4 on page 29.

FortiAnalyzer	• 5.4.0 to 5.4.4 • 5.2.0 to 5.2.11 • 5.0.0 to 5.0.13
FortiCache	• 4.2.2 • 4.1.2 • 4.0.0 to 4.0.4
FortiClient	• 5.4.3 • 5.4.1 • 5.2.0 and later
FortiMail	• 5.3.7 to 5.3.9 • 5.2.9 • 5.1.6 • 5.0.10
FortiSandbox	• 2.4.1 • 2.4.0 • 2.3.2 • 2.2.1 • 2.1.2 • 1.4.0 and later • 1.3.0 • 1.2.0 and 1.2.3
FortiSwitch ATCA	• 5.2.3 • 5.0.0 and later • 4.3.0 and later • 4.2.0 and later
FortiWeb	• 5.8.0 • 5.6.0 • 5.5.4 • 5.4.1 • 5.3.8 • 5.2.4 • 5.1.4 • 5.0.6

FortiDDoS	• 4.3.1 • 4.4.2 • 4.2.3 • 4.1.11 Limited support. For more information, see Feature support on page 17.
FortiAuthenticator	• 4.3.2

Virtualization	• Amazon Web Service AMI, Amazon EC2, Amazon EBS
	• Citrix XenServer 6.2
	• Linux KVM Redhat 6.5
	• Microsoft Azure
	• Microsoft Hyper-V Server 2008 R2, 2012 & 2012 R2
	• OpenSource XenServer 4.2.5
	• VMware
	  • ESX versions 4.0 and 4.1
	  • ESXi versions 4.0, 4.1, 5.0, 5.1, 5.5, 6.0 and 6.5

To confirm that a device model or firmware version is supported by current firmware version running on FortiManager, run the following CLI command:

```
diagnose dvm supported-platforms list
```

Always review the Release Notes of the supported platform firmware version before upgrading your device.

Feature support

The following table lists FortiManager feature support for managed platforms.

Platform	Management Features	FortiGuard Update Services	Reports	Logging
FortiGate	✓	✓	✓	✓
FortiCarrier	✓	✓	✓	✓
FortiAnalyzer			✓	✓
FortiCache			✓	✓

Platform	Management Features	FortiGuard Update Services	Reports	Logging
FortiClient		✓	✓	✓
FortiDDoS			✓	✓
FortiMail		✓	✓	✓
FortiSandbox		✓	✓	✓
FortiSwitch ATCA	✓			
FortiWeb		✓	✓	✓
FortiAuthenticator				✓
Syslog				✓

Language support

The following table lists FortiManager language support information.

Language	GUI	Reports
English	✓	✓
Chinese (Simplified)	✓	✓
Chinese (Traditional)	✓	✓
French		✓
Japanese	✓	✓
Korean	✓	✓
Portuguese		✓
Spanish		✓

To change the FortiManager language setting, go to *System Settings* > *Admin* > *Admin Settings*, in *Administrative Settings* > *Language* select the desired language on the drop-down menu. The default value is *Auto Detect*.

Russian, Hebrew, and Hungarian are not included in the default report languages. You can import language translation files for these languages via the command line interface using one of the following commands:

```
execute sql-report import-lang <language name> <ftp> <server IP address> <user name>
    <password> <file name>
```

```
execute sql-report import-lang <language name> <sftp <server IP address> <user name>
    <password> <file name>
execute sql-report import-lang <language name> <scp> <server IP address> <user name>
    <password> <file name>
execute sql-report import-lang <language name> <tftp> <server IP address> <file name>
```

For more information, see the *FortiManager CLI Reference*.

Supported models

The following tables list which FortiGate, FortiCarrier, FortiDDoS, FortiAnalyzer, FortiMail, FortiSandbox, FortiSwitch ATCA, FortiWeb, and FortiCache models and firmware versions that can be managed by a FortiManager or send logs to a FortiManager running version 5.4.4.

Software license activated LENC devices are supported, if their platforms are in the supported models list. For example, support of FG-3200D indicates support of FG-3200D-LENC.

FortiGate models

Model	Firmware Version
FortiGate: FG-30D, FG-30D-POE, FG-30E, FG-30E-3G4G-INTL, FG-30E-3G4G-NAM, FG-50E, FG-51E, FG-52E, FG-60D, FG-60D-POE, FG-60E, FG-60E-DSL, FG-60E-POE, FG-61E, FG-70D, FG-70D-POE, FG-80C, FG-80CM, FG-80D, FG-80E, FG-80E-POE, FG-81E, FG-81E-POE, FG-90D, FG-90D-POE,FG-90E, FG-91E, FG-92D, FG-94D-POE, FG-98D-POE, FG-100D, FG-100E, FG-100EF, FG-101E, FG-140D, FG-140E, FG-140D-POE, FG-140E-POE, FG-200D, FG-200D-POE, FG-240D, FG-240D-POE, FG-280D-POE, FG-200E, FG-201E, FGT-300D, FG-300E, FG-301E, FG-400D, FG-500D, FG-500E, FG-501E, FG-600C, FG-600D, FG-800C, FG-800D, FG-900D, FG-1000C, FG-1000D, FG-1200D, FG-1500D, FG-1500DT, FG-3000D, FG-3100D, FG-3200D, FG-3240C, FG-3600C, FG-3700D, FG-3700DX, FG-3810D, FG-3815D, FG-2000E, FG-2500E, FG 3800D, FG-3960E, FG-3980E, **FortiGate 5000 Series:** FG-5001C, FG-5001D, FG-5001E, FG-5001E1 **FortiGate 7000 Series:** FG-7030E-Q, FG-7030E-S, FG-7040E-1, FG-7040E-2, FG-7040E-3, FG-7040E-4, FG-7040E-5, FG-7040E-6, FG-7040E-8, FG-7040E-8-DC, FG-7060E-1, FG-7060E-2, FG-7060E-3, FG-7060E-4, FG-7060E-5, FG-7060E-6, FG-7060E-8 **FortiGate DC:** FG-80C-DC, FG-600C-DC, FG-800C-DC, FG-1000C-DC, FG-1500D-DC, FG-3000D-DC, FG-3100D-DC, FG-3200D-DC, FG-3240C-DC, FG-3600C-DC, FG-3700D-DC, FG-3800D-DC, FG-3810D-DC, FG-8000D-DC **FortiGate Low Encryption:** FG-80C-LENC, FG-100D-LENC, FG-600C-LENC, FG-1000C-LENC **FortiWiFi:** FWF-30D, FWF-30E, FWF-30E-3G4G-INTL, FWF-30E-3G4G-NAM, FWF-50E, FWF-50E-2R, FWF-51E, FWF-30D-POE, FWF-60D, FWF-60D-POE, FWF-60E-DSL, FWF-90D, FWF-90D-POE, FWF-92D, FWF-60E, FWF-61E, FWF-80CM, FWF-81CM **FortiGate VM:** FG-VM, FG-VM64, FG-VM64-AWS, FG-VM64-AWSONDEMAND, o FG-VM64-AZUREONDEMAND, FG-VM64-HV, FG-VM64-KVM, FG-VM64-XEN, FG-VMX-Service-Manager **FortiGate Rugged:** FGR-30D, FGR-35D, FGR-60D, FGR-90D	5.4

Model	Firmware Version
FortiGate: FG-20C, FG-20C-ADSL-A, FG-30D, FG-30D-POE, FG-40C, FG-60C, FG-60C-POE, FG-60C-SFP, FG-60D, FG-60D-3G4G-VZW, FG-60D-POE, FG-70D, FG-70D-POE, FG-80C, FG-80CM, FG-80D, FG-90D, FG-90D-POE, FG-92D, FG-94D-POE, FG-98D-POE, FG-100D, FG-110C, FG-111C, FG-140D, FG-140D-POE, FG-140D-POE-T1, FG-200B, FG-200B-POE, FG-200D, FG-200D-POE, FG-240D, FG-240D-POE, FG-280D-POE, FG-300C, FG-300D, FG-310B, FG-311B, FG-400D, FG-500D, FG-600D, FG-900D, FG-600C, FG-620B, FG-621B, FG-800C, FG-800D, FG-1000C, FG-1000D, FG-1200D, FG-1240B, FG-1500D, FG-1500DT, FG-3000D, FG-3016B, FG-3040B, FG-3100D, FG-3140B, FG-3200D, FG-3240C, FG-3600C,FG-3700D, FG-3700DX, FG-3810A, FG-3810D, FG-3815D, FG-3950B, FG-3951B **FortiGate 5000 Series:** FG-5001A, FG-5001A-SW, FG-5001A-LENC, FG-5001A-DW-LENC, FG-5001A-SW-LENC, FG-5001B, FG-5001C, FG-5001D, FG-5101C **FortiGate DC:** FG-80C-DC, FG-300C-DC, FG-310B-DC, FG-600C-DC, FG-620B-DC, FG-621B-DC, FG-800C-DC, FG-1000C-DC, FG-1240B-DC, FG-1500D-DC, FG-3000D-DC, FG-3040B-DC, FG-3100D-DC, FG-3140B-DC, FG-3200D-DC, FG-3240C-DC, FG-3600C-DC, G-3700D-DC, FG-3810A-DC, FG-3810D-DC, FG-3815D-DC, FG-3950B-DC, FG-3951B-DC, FG-8000D-DC **FortiGate Low Encryption:** FG-20C-LENC, FG-40C-LENC, FG-60C-LENC, FG-80C-LENC, FG-100D-LENC, FG-200B-LENC, FG-300C-LENC, FG-620B-LENC, FG-1000C-LENC, FG-1240B-LENC, FG-3040B-LENC, FG-310B-LENC, FG-600C-LENC, FG-3140B-LENC, FG-3810A-LENC, FG-3950B-LENC **FortiWiFi:** FWF-20C, FWF-20C-ADSL-A, FWF-30D, FWF-30D-POE, FWF-40C, FWF-60C, FWF-60CM, FWF-60CX-ADSL-A, FWF-60D, FWF-60D-3G4G-VZW, FWF-60D-POE, FWF-80CM, FWF-81CM, FWF-90D, FWF-90D-POE, FWF-92D **FortiGate Rugged:** FGR-60D, FGR-100C **FortiGate VM:** FG-VM-Azure, FG-VM, FG-VM64, FG-VM64-HV, FG-VM64-KVM, FG-VM64-XEN **FortiSwitch:** FS-5203B, FCT-5902D	5.2

Model	Firmware Version
FortiGate: FG-20C, FG-20C-ADSL-A, FG-30D, FG-30D-POE, FG-40C, FG-60C, FG-60C-POE, FG-60C-SFP, FG-60D, FG-60D-3G4G-VZW, FG-60D-POE, FG-70D, FG-70D-POE, FG-80C, FG-80CM, FG-80D, FG-90D, FG-90D-POE, FG-92D, FG-94D-POE, FG-98D-POE, FG-100D, FG-110C, FG-111C, FG-140D, FG-140D-POE, FG-140D-POE-T1, FG-200B, FG-200B-POE, FG-200D, FG-200D-POE, FG-240D, FG-240D-POE, FG-280D-POE, FG-300C, FG-300D, FG-310B, FG-311B, FG-500D, FG-600C, FG-620B, FG-621B, FG-700D, FG-800C, FG-900D, FG-1000C, FG-1000D, FG-1200D, FG-1240B, FG-1500D, FG-3000D, FG-3016B, FG-3040B, FG-3100D, FG-3140B, FG-3200D, FG-3240C, FG-3600C, FG-3700D, FG-3810A, FG-3950B, FG-3951B **FortiGate 5000 Series:** FG-5001A, FG-5001A-SW, FG-5001A-LENC, FG-5001A-DW-LENC, FG-5001A-SW-LENC, FG-5001B, FG-5001C, FG-5001D, FG-5101C **FortiGate DC:** FG-80C-DC, FG-300C-DC, FG-310B-DC, FG-600C-DC, FG-620B-DC, FG-621B-DC, FG-800C-DC, FG-1000C-DC, FG-1240B-DC, FG-1500D-DC, FG-3000D-DC, FG-3040B-DC, FG-3100D-DC, FG-3140B-DC, FG-3200D-DC, FG-3240C-DC, FG-3600C-DC, FG-3700D-DC, FG-3810A-DC, FG-3950B-DC, FG-3951B-DC **FortiGate Low Encryption:** FG-20C-LENC, FG-40C-LENC, FG-60C-LENC, FG-80C-LENC, FG-100D-LENC, FG-200B-LENC, FG-300C-LENC, FG-310B-LENC, FG-600C-LENC, FG-620B-LENC, FG-1000C-LENC, FG-1240B-LENC, FG-3040B-LENC, FG-3140B-LENC, FG-3810A-LENC, FG-3950B-LENC **FortiWiFi:**FWF-20C, FWF-20C-ADSL-A, FWF-30D, FWF-30D-POE, FWF-40C, FWF-60C, FWF-60CM, FWF-60CX-ADSL-A, FWF-60D, FWF-60D-POE, FWF-60D-3G4G-VZW, FWF-80CM, FWF-81CM, FWF-90D, FWF-90D-POE, FWF-92D **FortiGate Rugged:** FGR-60D, FGR-90D, FGR-100C **FortiGateVoice:** FGV-40D2, FGV-70D4 **FortiGate VM**: FG-VM, FG-VM64, FG-VM64-AWS, FG-VM64-AWSONDEMAND, FG-VM64-HV, FG-VM64-KVM, FG-VM64-XEN **FortiSwitch:** FS-5203B	5.0

FortiCarrier Models

Model	Firmware Version
FortiCarrier: FCR-3000D, FCR-3100D, FCR-3200D, FCR-3700D, FCR-3700DX, FCR-3800D, FCR-3810D, FCR-3815D, FCR-5001C, FCR-5001D, FCR-3000D-DC, FCR-3100D-DC, FCR-3200D-DC, FCR-3240C, FCR-3600C, FCR-3700D-DC, FCR-3810D-DC, FCR-5001C **FortiCarrier DC:** FCR-3000D-DC, FCR-3100D-DC, FCR-3200D-DC, FCR-3240C-DC, FCR-3600C-DC, FCR-3700D-DC, FCR-3800D-DC, FCR-3810D-DC, FCR-3815D-DC **FortiCarrier VM:** FCR-VM, FCR-VM64, FCR-VM64-AWS, FCR-VM64-AWSONDEMAND, FCR-VM64-HV, FCR-VM64-KVM	5.4
FortiCarrier: FCR-3000D, FCR-3100D, FCR-3200D, FCR-3240C, FCR-3600C, FCR-3700D, FCR-3700DX, FCR-3810A, FCR-3810D, FCR-3815D, FCR-3950B, FCR-3951B, FCR-5001A, FCR-5001B, FCR-5001C,FCR-5001D, FCR-5101C, FCR5203B, FCR-5902D **FortiCarrier DC:** FCR-3000D-DC, FCR-3100D-DC, FCR-3200D-DC, FCR-3700D-DC, FCR-3810D-DC **FortiCarrier Low Encryption:** FCR-5001A-DW-LENC **FortiCarrier VM:** FCR-VM, FCR-VM64, FCR-VM64-HV, FCR-VM64-KVM, FCR-Vm64-XEN, FCR-VM64-AWSONDEMAND	5.2
FortiCarrier: FCR-3240C, FCR-3600C, FCR-3810A, FCR-3950B, FCR-3951B, FCR-5001A, FCR-5001B, FCR-5001C, FCR-5001D, FCR-5101C **FortiCarrier DC:** FCR-3240C-DC, FCR-3600C-DC, FCR-3810A-DC, FCR-3950B-DC, FCR-3951B-DC **FortiCarrier Low Encryption:** FCR-5001A-DW-LENC **FortiCarrier VM:** FCR-VM, FCR-VM64	5.0

FortiDDoS models

Model	Firmware Version
FortiDDoS: FI-200B, FI400B, FI-600B, FI-800B, FI-900B, FI-1000B, FI-1200B, FI-2000B, FI-3000B	4.2, 4.1, 4.0

FortiAnalyzer models

Model	Firmware Version
FortiAnalyzer: FAZ-200D, FAZ-300D, FAZ-400E, FAZ-800F, FAZ-1000C, FAZ-1000D, FAZ-1000E, FAZ-2000B, FAZ-2000E, FAZ-3000D, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, FAZ-3900E, and FAZ-4000B. **FortiAnalyzer VM:** FAZ-VM64, FMG-VM64-Azure, FAZ-VM64-HV, FAZ-VM64-XEN (Citrix XenServer and Open Source Xen), FAZ-VM64-KVM, and FAZ-VM64-AWS.	5.4
FortiAnalyzer: FAZ-100C, FAZ-200D, FAZ-300D, FAZ-400C, FAZ-400E, FAZ-1000C, FAZ-1000D, FAZ-1000E, FAZ-2000B, FAZ-3000D, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, FAZ-3900E, FAZ-4000B **FortiAnalyzer VM:** FAZ-VM, FAZ-VM-AWS, FAZ-VM64, FAZ-VM64-Azure, FAZ-VM64-HV, FAZ-VM64-KVM, FAZ-VM64-XEN	5.2
FortiAnalyzer: FAZ-100C, FAZ-200D, FAZ-300D, FAZ-400B, FAZ-400C, FAZ-400E, FAZ-1000B, FAZ-1000C, FAZ-1000D, FAZ-1000E, FAZ-2000A, FAZ-2000B, FAZ-3000D, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, FAZ-4000A, FAZ-4000B **FortiAnalyzer VM:** FAZ-VM, FAZ-VM64, FAZ-VM64-AWS, FAZ-VM64-Azure, FAZ-VM64-HV, FAZ-VM-KVM, FAZ-VM-XEN	5.0

FortiMail models

Model	Firmware Version
FortiMail: FE-60D, FE-200D, FE-200E, FE-400C, FE-400E, FE-1000D, FE-2000B, FE-2000E, FE-3000C, FE-3000D, FE-3000E, FE-3200E, FE-5002B **FortiMail Low Encryption:** FE-3000C-LENC **FortiMail VM:** FE-VM64, FE-VM64-HV, FE-VM64-XEN	5.3.7
FortiMail: FE-60D, FE-200D, FE-200E, FE-400C, FE-400E, FE-1000D, FE-2000B, FE-3000C, FE-3000D, FE-5002B **FortiMail VM:** FE-VM64, FE-VM64-HV, FE-VM64-XEN	5.2.8
FortiMail: FE-100C, FE-200D, FE-200E, FE-400B, FE-400C, FE-400E, FE-1000D, FE-2000B, FE-3000C, FE-3000D, FE-5001A, FE-5002B **FortiMail VM:** FE-VM64	5.1.6
FortiMail: FE-100C, FE-200D, FE-200E, FE-400B, FE-400C, FE-1000D, FE-2000A, FE-2000B, FE-3000C, FE-3000D, FE-4000A, FE-5001A, FE-5002B **FortiMail VM:** FE-VM64	5.0.10

FortiSandbox models

Model	Firmware Version
FortiSandbox: FSA-1000D, FSA-3000D, FSA-3000E, FSA-3500D **FortiSandbox VM:** FSA-VM	2.3.2
FortiSandbox: FSA-1000D, FSA-3000D, FSA-3500D **FortiSandbox VM:** FSA-VM	2.2.0 2.1.0
FortiSandbox: FSA-1000D, FSA-3000D **FortiSandbox VM:** FSA-VM	2.0.0 1.4.2
FortiSandbox: FSA-1000D, FSA-3000D	1.4.0 and 1.4.1 1.3.0 1.2.0 and later

FortiSwitch ACTA models

Model	Firmware Version
FortiController: FTCL-5103B, FTCL-5902D, FTCL-5903C, FTCL-5913C	5.2.0
FortiSwitch-ATCA: FS-5003A, FS-5003B **FortiController:** FTCL-5103B, FTCL-5903C, FTCL-5913C	5.0.0
FortiSwitch-ATCA: FS-5003A, FS-5003B	4.3.0 4.2.0

FortiWeb models

Model	Firmware Version
FortiWeb: FWB-2000E	5.6.0
FortiWeb: FWB-100D, FWB-400C, FWB-400D, FWB-1000C, FWB-1000D, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-3010E, FWB-4000C, FWB-4000D, FWB-4000E **FortiWeb VM:** FWB-VM-64, FWB-XENAWS, FWB-XENOPEN, FWB-XENSERVER, FWB-HYPERV, FWB-KVM, FWB-AZURE	5.5.3

Model	Firmware Version
FortiWeb: FWB-100D, FWB-400C, FWB-1000C, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-4000C, FWB-4000D, FWB-4000E **FortiWeb VM:** FWB-VM64, FWB-XENAWS, FWB-XENOPEN, FWB-XENSERVER, FWB-HYPERV	5.4.1
FortiWeb: FWB-100D, FWB-400B, FWB-400C, FWB-1000B, FWB-1000C, FWB-1000D, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-4000C, FWB-4000D, FWB-4000E **FortiWeb VM:** FWB-VM64, FWB-XENAWS, FWB-XENOPEN, FWB-XENSERVER, and FWB-HYPERV	5.3.8
FortiWeb: FWB-100D, FWB-400B, FWB-400C, FWB-1000B, FWB-1000C, FWB-1000D, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-4000C, FWB-4000D, FWB-4000E **FortiWeb VM:** FWB-VM64, FWB-HYPERV,FWB-XENAWS, FWB-XENOPEN, FWB-XENSERVER	5.2.4

FortiCache models

Model	Firmware Version
FortiCache: FCH-400C, FCH-400E, FCH-1000C, FCH-1000D, FCH-3000C, FCH-3000D, FCH-3000E, FCH-3900E **FortiCache VM:** FCH-VM64, ForiCache-KVM	4.1
FortiCache: FCH-400C, FCH-400E, FCH-1000C, FCH-1000D, FCH-3000C, FCH-3000D, FCH-3900E **FortiCache VM:** FCH-VM64	4.0

FortiAuthenticator models

Model	Firmware Version
FortiAuthenticator: FAC-200D, FAC-200E, FAC-400C, FAC-400E, FAC-1000C, FAC-1000D, FAC-3000B, FAC-3000D, FAC-3000E, FAC-VM	4.0 and 4.1

Compatibility with FortiOS Versions

This section highlights compatibility issues that administrators should be aware of in 5.4.4.

Compatibility issues with FortiOS 5.4.8

The following table lists interoperability issues that have been identified with FortiManager version 5.4.4 and FortiOS 5.4.8.

Bug ID	Description
469700	FortiManager is missing three wtp-profiles: FAP221E, FAP222E, and FAP223E.

Compatibility issues with FortiOS 5.4.5

The following table lists interoperability issues that have been identified with FortiManager version 5.4.4 and FortiOS 5.4.5.

Bug ID	Description
434637	FortiGate `config ssd-trim-freq` causes FortiManager retrieval failure.
417581	AP Profile in AP Manager missing AP Country Code for TZ (Tanzania).

Compatibility issues with FortiOS 5.4.4

The following table lists interoperability issues that have been identified with FortiManager version 5.4.4 and FortiOS 5.4.4.

Bug ID	Description
407566	The *accesspoint-name* of an extended controller is lost when name contains more than thirty one characters.
407577	FortiManager should support the following syntax: `gui-domain-ip-reputation` and `auth-multi-group`.
407579	FortiManager should support the CLI, `ipsec-dec-subengine-mask`, on platforms that equip with the NP6 chipset.

Compatibility issues with FortiOS 5.2.10

The following table lists interoperability issues that have been identified with FortiManager version 5.4.4 and FortiOS 5.2.10.

Bug ID	Description
397220	FortiOS 5.2.10 increased the maximum number of the firewall schedule objects for 1U and 2U+ appliances. As a result, a retrieve may fail if more than the maximum objects are configured.

Compatibility issues with FortiOS 5.2.7

The following table lists interoperability issues that have been identified with FortiManager version 5.4.4 and FortiOS 5.2.7.

Bug ID	Description
365757	Retrieve may fail on LDAP User Group if object filter has more than 511 characters.
365766	Retrieve may fail when there are more than 50 portals within a VDOM.
365782	Install may fail on system global optimize or system fips-cc entropy-token.

Compatibility issues with FortiOS 5.2.6

The following table lists interoperability issues that have been identified with FortiManager version 5.4.4 and FortiOS 5.2.6.

Bug ID	Description
308294	1) New default wtp-profile settings on FOS 5.2.6 cause verification errors during installation. 2) FortiManager only supports 10,000 firewall addresses while FortiOS 5.2.6 supports 20,000 firewall addresses.

Compatibility issues with FortiOS 5.2.1

The following table lists interoperability issues that have been identified with FortiManager version 5.4.4 and FortiOS version 5.2.1.

Bug ID	Description
262584	When creating a VDOM for the first time it fails.
263896	If it contains the certificate: `Fortinet_CA_SSLProxy` or `Fortinet_SSLProxy`, `retrieve` may not work as expected.

Compatibility issues with FortiOS 5.2.0

The following table lists known interoperability issues that have been identified with FortiManager version 5.4.4 and FortiOS version 5.2.0.

Bug ID	Description
262584	When creating a VDOM for the first time it fails.
263949	Installing a VIP with port forwarding and ICMP to a 5.2.0 FortiGate fails.

Compatibility issues with FortiOS 5.0.5

The following table lists known interoperability issues that have been identified with FortiManager version 5.2.1 and FortiOS version 5.0.5.

Bug ID	Description
230199	FortiManager allows the creation of a new FAP-320C WTP profile on a FortiOS 5.0.5 device causing the install to fail. FAP-320C is new for FortiOS 5.0.6.

Compatibility issues with FortiOS 5.0.4

The following table lists known interoperability issues that have been identified with FortiManager version 5.4.4 and FortiOS version 5.0.4.

Bug ID	Description
226064	Attempting to install time zones 79 and 80 fails. These time zones were added in FortiOS 5.0.5.
226078	When the password length is increased to 128 characters, the installation fails.
226098	When installing a new endpoint-control profile, installation verification fails due to default value changes in FortiOS 5.0.5.
226102	If DHCP server is disabled, installation fails due to syntax changes in FortiOS 5.0.5.

Bug ID	Description
226203	Installation of address groups to some FortiGate models may fail due to table size changes. The address group table size was increased in FortiOS 5.0.5.
226236	The `set dedicated-management-cpu enable` and `set user-anonymize enable` CLI commands fail on device install. These commands were added in FortiOS 5.0.5.
230199	FortiManager allows the creation of a new FAP-320C WTP profile on a FortiOS 5.0.4 device causing the install to fail. FAP-320C is new for FortiOS 5.0.6.

Resolved Issues

The following issues have been fixed in 5.4.4. For inquires about a particular bug, please contact Customer Service & Support.

Device Manager

Bug ID	Description
249922	Exported Device List does not contain HA information for devices.
302342	Enabling *Allow Push Update* in FortiGuard Distribution Network may not work from the GUI.
372581	`dns-service` is set to local if users set the *Use System DNS* setting from GUI.
397151	Users may be forced to select an admin profile when creating a Restricted Admin to Guest Account Provisioning Only.
399254	Users may see Relay Service from other VDOM's when they are configuring DHCP Server in the Device Manager.
404708	Installations may fail due to outdated FAP200A default wireless profile.
412494	Hostnames may not be shown in Detected Devices.
414429	FortiManager may unset `switch-controller` when FortiSwitch is being managed.
416266	Changes of PAC file in *System : Explicit Proxy* may not be saved.
416529	`ip-pools` in SSL VPN portal profiles may not be pushed to FortiGate.
417195	FortiManager may be slow to respond when there are many FortiExtenders attached to the managed FortiGates
417200	`engine-id` under `config system snmp sysinfo` may not be installed to FortiGate.
421866	`block intra-zone traffic` setting may be lost after users remove an interface from an ADOM interface mapping.
434285	The replaced device may not enter the Unregistered Device List.
434847	Users may not be able to select some interface in *Listen on Interfaces* for explicit proxy from the GUI.

Bug ID	Description
437583	*Connect to CLI via* may connect to the same device if there are multiple FortiGates behind NAT.
441237	Users may fail to create a DHCP relay server with a VLAN interface.
441649	Users may fail to enable SNMPv3 in provisioning template for 5.2 ADOMs.
441878	The option *both* may be unavailable for *authtype in system -> lte-modem*.
442532	It may be slow to connect to FortiGate CLI from Device Manager Dashboard.
445688	Retrieving configuration from FortiGate may fail due to duplicate `webfilter url-filter` entries.
446637	Interface attributes `l2forward`, `ipmac` and `subst` may be unset during installation.
447063	Installation may fail if the `md5-key` contains a comma in OSPF settings.
448289	The category *Multicast address6* may not be displayed correctly in import conflicts page.
451737	Adding a FortiGate may fail if there is invalid datasource on FortiGate.
435256	Add a CLI and GUI option to restrict contact to the FortiGuard server in US locations only.

Global ADOM

Bug ID	Description
421773	Global policy package assignment may get stuck at 70% on a FortiManager with multiple CPUs.
435322	Web filter override changes in Global ADOM may not trigger the *Assign* feature for policy packages.
438641	Adding an ADOM to Policy Package assignment page may cause the other ADOMs status to be changed to *Pending* changes.
438643	-Users may fail to clone a policy package in Global ADOM if its name starts with *Global*.
439743	Excluding one Policy Package in Global ADOM assignment page may cause Policy Package status in other ADOMs to be modified.
440107	Global ADOM may fail to be upgraded if there are invalid dynamic mappings.

Bug ID	Description
448616	Deleting a Global policy may not be updated to assigned ADOMs.

Policy and Objects

Bug ID	Description
167355	Default object colors on FortiManager may not match the ones on FortiGate.
293781	FortiManager may not support policy hit count reset.
355180	Users may not be brought back to the Duplicate Objects page after a merge operation.
357218	Users may not be able to reorder Static URL filter in Web Filter profile.
366996	Sometimes install preview may show incorrect content when users are installing several policy packages.
376516	Users cannot choose *Suspicious Files Only for AntiVirus Profile* in FortiManager from GUI.
376655	Installation may fail because FortiManager tries to unset `client-cert-request` setting in the *ssl-ssh-profile*.
380522	`fsso-polling objects` may get deleted during installation.
389515	Users may not be able to edit or delete a service category with `&` in its name.
392443	Setting `quarantine-expiry` for IPS sensor from FortiManager may cause installation fail.
393077	Setting a *global-label* for one policy may also apply it to all policies below it.
401487	Sometimes GUI displays *Nothing to install* while the installation task is running.
401843	Insert policy above/below may create a duplicate section.
402685	Copy error may occur if users are using a local certificate with global range from a VDOM.
406781	Search may not work in LDAP user objects.
411896	Users may not be able to update `fsso` correctly from GUI.
416099	Tags may not be displayed.
417443	Adding users from OpenLDAP and eDirectory LDAP may be failed.

Bug ID	Description
422847	FortiManager may return an error when editing or cloning a zone that has a large number of interface members.
423757	A wildcard URL entry with action block may be moved to the first in the URL Filter list in Web Filter profile.
433623	The Policy Interface Pair View may not pair properly and duplication may occur.
433866	Installation may be blocked if a Zone Name is the same as a member Interface Name.
434671	When users try to add a new device to *Installation Target* via *Search* function in the GUI, it may remove all existing installation targets.
435211	IPS custom signatures with `-crc32` may not be created in FortiManager.
435320	Search may not work for imported Dynamic Address Objects that are imported within a Dynamic Address Group.
435971	URL filter rules may be re-ordered following a FortiManager upgrade.
435971	The order of URL filter rules may be changed after FortiManager upgrade.
436421	Policy Object Selector Panel enhancements.
436676	Users may not be able to create or copy and paste Explicit Proxy Policies.
436886	Updating a policy may take a long time if there are many policies.
437238	Sometimes Web Filter may display web elements.
438497	After users paste a policy below another one, the page may automatically scroll to the top.
438584	Import policies may get stuck if there is a firewall address with an empty address type.
439047	Policy hit count may be also copied if users copy and paste a policy.
439086	The sequence number of a policy may be changed after users drag an object to a column.
439356	Not all groups may be displayed when users try to assign a user device to a group.
439594	Users may be unable to delete duplicated dynamic mappings.
439749	Deleting a Dynamic Mapping of an object may cause status of other Policy Packages referencing this object to be *Modified*.
439942	The filter function for IPS signatures may not work.
440266	Users may not be able to delete Source Address *All* from explicit proxy policies.

Bug ID	Description
440317	Deleting a device in Dynamic Mappings for Zone may cause Policy Package status to be *Modified*.
442769	Installation preview may get stuck at 15% following the FortiManager upgrade.
443564	Firewall Policy may not be displayed after it is created.
444304	`Server-cert` may not be applied to the `ssl-ssh-profile`.
444316	Importing a Dynamic Mapping of firewall address for a VDOM other than root may fail.
444709	The default HTTPS port number may be `433` in SSL/SSH Inspection profile.
445010	LDAP users containing escape characters `\` may not be displayed properly.
446026	Policy check process may get stuck at 25%.
446245	FortiManager may still update objects even if users choose *Keep value from FMG* during policy import.
447674	The order of customer service may change during policy import.
448113	ADOM revision diff may show difference when two revisions are identical.
449000	Some fields may be missing in exported policy package files.
449533	FortiManager may fail to import a URL filter with an apostrophe.
450092	Custom IPS signatures with `!` in the `--pcre field` may not be accepted by FortiManager.
450430	When the last object is removed in a field, it may become empty.
452022	Policy package status may not change to *Modified* after updating a firewall address object being used in the policy package.
4381701	When users create customer service and set an `iprange`, `set fqdn` may be used instead of `set iprange`.

Script

Bug ID	Description
401486	Running a TCL script may be reported as successful from GUI while the device password is incorrect.

Bug ID	Description
407797	Users may not be able to set a weekly schedule in per Device Script History page.
411361	Running a script on both a group and a single device may hang.
435105	When `allow-subnet-overlap` is enabled, users may not be able to set up an overlapping IP address and subnet on the interface and the IPSec tunnel interface by running the CLI script.
444976	*Import Script* function may not be displayed in the top toolkit.

Services

Bug ID	Description
400982	Too many FortiClient update requests may cause the UDM to stop working.
418535	`fds_svrd` may take up to 100% CPU.
437194	Sometimes FortiManager may still connect directly to the servers from the FDS list although there are FDS proxy settings configured.
440718	If an FOSVM joins a HA cluster as a slave when it is in the Unregistered Device List, it may not be able to get the UTM contract from FortiManager.

System Settings

Bug ID	Description
381189	Event log may not be generated for an admin password change.
394218	Admin profiles may not include Global Database in ADOM scope options.
416505	Policy &Packages, AP Manager and FortiSwitch modules may not be accessible to Remote Radius admin users.
417616	Daylight saving time for Moscow time zone may not work properly.
422627	Scheduled backup to SFTP server may fail.
438586	The landing page for Restricted Admin may be different each time he logs in.

Bug ID	Description
439377	Duplicate event log entries may be generated for changes made on FortiManager HA master.
443717	Syslog server1 may be allowed to be deleted.

VPN Management

Bug ID	Description
437750	The error message is not clear when users try to add more than 10 portals.
441512	Users may not be able to use nested address groups as protected subnets.
445172	Some fields may be missing in cloned IPSec Phase1/Phase2.

VPN Manager

Bug ID	Description
356454	SSL VPN monitor may show information for VDOMs managed by other ADOMs.
400529	Changing node settings may not trigger installation when workspace is enabled and installation target is a group.
417007	Changing `remote-gw` may delete and re-configure FortiGate VPNs.
441646	Users may not be able to install the configurations to Spoke if they only make changes in the Hub.

AP Manager

Bug ID	Description
397342	Users may not be able to change the encrypt or disable WiFi broadcast in the AP Manager WiFi templates.
434610	Channel Width may be saved as 20MHz for 802.11ac/n radio and 802.11ac radio in the AP profile.

Bug ID	Description
442114	Change of administrative access on WiFi Templates may change the SSID DHCP lease-time.
439365	*Schedule* may be missing in AP Manager SSID configuration page.
440650	Users may not be able to configure multiple DNS servers in SSID profile.

Workplace and WorkFflow

Bug ID	Description
418195	When the Workspace Mode is enabled, the GUI may hang after users switch from Global ADOM to other ADOMs.
438424	Admin user may not be able to approve sessions in Workflow Mode.
434642	`execute fmpolicy promote-adom-object` may not work properly in Workflow Mode.
423315	The *Save* button may be triggered for a locked policy package.
435083	Users are able to quick edit *Comment* without locking the ADOM.

Others

Bug ID	Description
378830	ADOM upgrade from v5.2 to v5.4 may fail because of DNS-based web-filtering profile.
401014	Apache being down intermittently may block access to GUI through HTTP or HTTPS.
414830	Corrupted images may be accepted for upgrade.
422425	Upgrading ADOM from v5.2 to v5.4 may fail because of `tcp-portrange` syntax problems.
437078	An ADOM may not be able to be deleted because of obsolete scripts.
442695	Slave FortiGate may be incorrectly counted as one device for licensing purposes.
452464	There may be too many logs generated for Policy Hit Count.

Common Vulnerabilities and Exposures

Bug ID	Description
442206	FortiManager 5.4.4 is no longer vulnerable to the following CVE-Reference: • 2017-9765 Visit https://fortiguard.com/psirt for more information.

Known Issues

The following issues have been identified in 5.4.4. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

AP Manager

Bug ID	Description
450434	FortiManager may try to unset `wtp-mode` if the `wtp-mode` is set to *remote*.

Device Manager

Bug ID	Description
395060	Discovery of LENC devices failed.
443766	Policy package status may still be *Modified* after an installation. **Workaround:** Use the command `diagnose cdb check policy-packages`.
449439	Some configuration may get removed during an installation if the database has been corrupted. **Workaround:** Perform a retrieve for that device in Device Manager.
451796	*Upgrade Firmware Task* may show Image upgrade failed while it has succeed.
453942	FortiManager may not be able to import an `ssl-ssh-profile` and return the error: *server-cert can not be changed when server-cert-mode is re-sign* **Workaround:** Please rename the affected `ssl-ssh-profile` on FortiGate, and perform a retrieve and run import wizard again on FortiManager.

Logging

Bug ID	Description
369270	FMG Slave may stop receiving FGT logs after changing device name **Workaround:** `restart oftpd on FMG slave` using command `dia test application oftpd 99`, after that oftp connections can be established and FMG slave can receive logs again from the FGT.

Policy & Objects

Bug ID	Description
453371	After Object Selector is set to *Dock to Bottom*, GUI may not be able to render policies on a refresh. **Workaround**: Please use *Dock to Right* option or the *Dual Pane* mode instead. You must enable the *Dual Pane* mode on the *System Settings* > *Advanced* > *Advanced Settings* pane before you can use it.

Revision History

Bug ID	Description
450711	After upgrading FortiManager to v5.4.4, installing FortiGate devices may fail due to verification errors on system resource limits. **Workaround:** Please run a retrieve on the affected FortiGate devices. Alternatively, users can specify a value on the erroneous system resource limit.

Services

Bug ID	Description
449797	The ratings of a website may be different when it starts with `http` or `https`.

FortiGuard Distribution Servers (FDS)

In order for the FortiManager to request and retrieve updates from FDS, and for FortiManager to serve as a FDS, please configure the necessary settings on all devices between FortiManager and FDS, or between FortiManager and FortiGate devices based on the items listed below:

- FortiManager accesses FDS for antivirus and attack updates through TCP/SSL port 443.
- If there is a proxy server between FortiManager and FDS, FortiManager uses port 80 to communicate with the proxy server by default and connects to the proxy server using HTTP protocol.
- If FortiManager manages a FortiGate device located behind a proxy server, the proxy server permits TCP/SSL traffic to pass through via port 443.

FortiGuard Center update support

You can configure FortiManager as a local FDS to provide FortiGuard updates to other Fortinet devices and agents on your network. The following table lists which updates are available per platform/version:

Platform	Version	Antivirus	AntiSpam	Vulnerability Scan	Software
FortiClient (Windows)	• 5.0.0 and later • 5.2.0 and later • 5.4.0 and later • 5.6.0 and later	✓		✓	
FortiClient (Windows)	• 4.3.0 and later	✓			
FortiClient (Windows)	• 4.2.0 and later	✓	✓		✓
FortiClient (Mac OS X)	• 5.0.1 and later • 5.2.0 and later	✓		✓	
FortiMail	• 4.2.0 and later • 4.3.0 and later • 5.0.0 and later • 5.1.0 and later • 5.2.0 and later • 5.3.7 to 5.3.9	✓	✓		

Platform	Version	Antivirus	AntiSpam	Vulnerability Scan	Software
FortiSandbox	• 1.2.0, 1.2.3 • 1.3.0 • 1.4.0 and later • 2.1.2 • 2.2.1 • 2.3.2	✓			
FortiWeb	• 5.0.6 • 5.1.4 • 5.2.0 and later • 5.3.0 • 5.4.1 • 5.5.4 • 5.6.0 • 5.8.0	✓			

To enable FortiGuard Center updates for FortiMail version 4.2 enter the following CLI command:

```
config fmupdate support-pre-fgt-43
   set status enable
end
```

FORTINET®

High Performance Network Security